The Heritage Foundation

BACKGROUNDER
No. 3757 | MARCH 22, 2023
TECHNOLOGY POLICY CENTER

TikTok Generation: A CCP Official in Every Pocket

Kara Frederick

KEY TAKEAWAYS

TikTok's data exploitation practices, privacy abuses, influence operations, and promotion of social contagions leave Americans vulnerable to the CCP.

Given the current threat environment, a wholesale ban of TikTok's operations in the U.S. is the only viable option to protect the United States and Americans.

A systemic, risk framework applied to foreign-owned platforms will prevent another TikTok from infiltrating America.

Three hundred billion dollars, three billion downloads, and at least 90 minutes of attention per user every day—TikTok and its China-based parent company have captured much of the world in more ways than one.[1] Yet today's most popular social media app poses a distinct threat to American citizens. From logging keystrokes to laundering pro–Chinese Communist Party (CCP) narratives to U.S. audiences, TikTok—via its Beijing-based parent company ByteDance—exposes Americans to a host of abuses by the Chinese government.

TikTok's data-collection and exploitation practices, abuses of privacy, propagation of influence operations, and promotion of social contagions that rend America's social fabric require immediate attention from policymakers. If America is to preserve her

self-governing republic, especially in the psyches of the next generation, dealing with TikTok and successor platforms is both a strategic and moral imperative.

TikTok and the CCP

TikTok's parent company, ByteDance, is subject to the People's Republic of China's (PRC) laws and policies that permit the CCP's access to the data ByteDance collects. One such policy is China's 2017 National Intelligence Law, which compels private entities and individuals to cooperate with "state intelligence work."[2] Specifically, Article 7 of this law declares that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to the law."[3]

Beyond this, Chinese officials—former and current—are embedded in TikTok's parent company and involved in the company's inner workings.[4] In April 2021, the Chinese government acquired a 1 percent stake in ByteDance's main domestic subsidiary and the board seat that came along with it. This action makes at least one of the three board members, Wu Shugang, a card-carrying official of the Chinese government.[5] Further, a U.S. Department of Justice filing against TikTok assessed in September 2020 that "ByteDance contains an internal corporate CCP committee through which the CCP exercises influence at the company."[6] At lower levels, an August 2022 *Forbes* review found more than 300 LinkedIn profiles of current TikTok and ByteDance employees with ties to the Chinese state media apparatus.[7] Fifteen of these profiles indicate that these professionals are both employed by ByteDance and official Chinese propaganda arms at the same time.[8]

In fact, TikTok's ties to the CCP via ByteDance are so deep that TikTok's public relations strategy from leaked documents published by *Gizmodo* in July 2022 in a document titled, "TikTok Master Messaging," include imperatives to "[d]ownplay the parent company ByteDance, downplay the China association," as two of the first four exhortations on the list.[9]

TikTok's Data Privacy and Collection Methods

While a number of private American platforms engage in controversial data-collection and tracking practices, TikTok's CCP links intensify debates over privacy invasion. Given its influence over the app, the CCP would likely encourage more collection, not less. And while the commercial surveillance practices of many American

companies are exploitative, direct comparisons do not account for the differences in corporate governance between American and Chinese companies as well as the stark contrasts between U.S. and Chinese political systems. America—though under internal pressure—retains a relatively open society, free press, engaged citizenry, and independent judiciary to hold both the U.S. government and private companies accountable for their data-collection practices.[10] China does not have a remotely comparable approach.

As of today, TikTok's invasive data-collection practices include gathering users' Global Positioning System (GPS) locations, Internet protocol (IP) addresses, content, contacts, images, microphone access (for "voiceprints"), and other biometric, personally identifiable, or device information.[11] Its 2023 Privacy Policy also includes admissions that TikTok collects the mobile carriers, time zone settings, models, networks, device identifiers, screen resolution, operating systems, app and file names and types, along with keystroke patterns or rhythms of its users.[12]

In terms of comparative data-collection practices to other platforms, a February 2023 report by cybersecurity company Internet 2.0 alleges that TikTok's data-collection behaviors are among the worst in the industry.[13] For example, TikTok's Malcore (malware analysis tool) score was 63.1 out of 100, the highest and worst score of the more than 20 digital applications it tested. The average application's score was 28.8, with no other app ranking as poorly in terms of data privacy and security as TikTok. According to the report, TikTok's performance was due, in part, to the security vulnerabilities in TikTok's code and the abundance of data trackers riddling the platform.[14]

Particularly troubling is the extent to which TikTok conceals atypical elements of its collection practices. In August 2020, *The Wall Street Journal* revealed that TikTok exploited a loophole in Google's Android operating system that allowed it to track the media access control (MAC) addresses (the unique device identifiers) of its users for at least 15 months. When TikTok was first installed on a new device over that time period, the company reportedly bundled these identifiers and other device data to send to parent company ByteDance.[15] During the 15-month period, TikTok reportedly took steps to cover its tracks and conceal its exploitation of this loophole via a layer of encryption.[16] TikTok also reportedly accessed user clipboards on Apple's mobile operating system for a time, reading the clipboard in every instance the app was opened, potentially exposing sensitive information, such as passwords and banking information, to TikTok.[17]

Whose Data? Everyone's Data

Hard security concerns, such as vulnerability to intrusion and hacking through lax security measures, backdoors, and even bugdoors (security flaws hidden in a programming vulnerability—wittingly or unwittingly) are present whenever a device connects to the Internet. Yet TikTok appears to have deliberately engineered access to non-public datasets for certain individuals. Leaked audio of 80 internal TikTok meetings obtained by *Buzzfeed* captured an external auditor as he mused: "I feel like with these tools, there's some backdoor to access user data in almost all of them."[18] If not backdoors, bugdoors can be introduced later via a software update that can provide access to certain systems. Additionally, TikTok could serve as a potential entry point to access the data of other people using the same Wi-Fi network.[19]

This matters because China-based engineers employed by ByteDance reportedly accessed U.S. user data multiple times over the course of at least four months from 2021 to 2022.[20] In June 2022, the same *Buzzfeed*-obtained leaked audio from TikTok's internal company meetings confirmed that China-based engineers accessed U.S. user information that was not public, to include birthdays and phone numbers.[21] Before that, TikTok's former chief information security officer tacitly admitted that employees in China had access to U.S. user data in a blog post in 2020.[22]

Separate whistleblower leaks point to access of U.S. user data by China-based employees as a pervasive practice among ByteDance employees. In a March 2023 letter to Committee on Foreign Investment in the United States (CFIUS) chair Janet Yellen, Senator Josh Hawley (R–MO) wrote that a former ByteDance employee with direct knowledge of TikTok's operations admitted that his colleagues could "switch between Chinese and U.S. data with nothing more than the click of a button using a proprietary tool...just like a light switch."[23] In this case, extensive safeguards to shield U.S. user data likely did not exist and it was not difficult for ByteDance employees to access the data of Americans at will. In 2022, ByteDance conceded that it built an entire initiative centered around using TikTok to monitor the locations of at least two U.S. journalists.[24] Known as Project Raven internally, this effort to track the physical locations of Americans was approved by ByteDance employees in China, likely as an attempt to ferret out the employees that leaked to *Buzzfeed* in the summer of 2022.[25]

Beyond access to data, the CCP's likely control over TikTok's algorithm—originally designed using ByteDance's algorithms and artificial intelligence (AI) models—raises questions about the app's potential

to be actively manipulated by CCP-linked actors.[26] During divestment talks with Oracle in 2020, ByteDance representatives reportedly indicated that they would not surrender TikTok's source code to the U.S. company and would instead retain it in China.[27] After all, the CCP would have much to lose if ByteDance transferred the algorithm to an American company. FBI Director Christopher Wray appeared to explain why in a public speech more than two years later, asserting that the Chinese government both controls ByteDance and has the "ability to control the recommendation algorithm."[28] In a later hearing in front of the Senate Intelligence Committee in 2023, Director Wray testified that the Chinese government could control the software and data of millions of users who have TikTok on their devices, as well as spread propaganda within America.[29] Given the CCP's authoritarian track record, it is naive to believe that it has not taken advantage of these capabilities.

Manipulating the Information Environment

Concerns over data security do not scratch the surface of TikTok's ability to manipulate the information environment. ByteDance and TikTok have already pushed pro-CCP narratives to the U.S. public, censored content of which the party-state disapproves, and gathered the necessary information to conduct tailored influence campaigns. In two years, the percentage of adults who get their news from TikTok on a regular basis rose from only 3 percent in 2020 to 10 percent of American adults in 2022—roughly tripling this audience.[30] Now, nearly a quarter of adults in the United States under the age of 30 claim to regularly get their news from TikTok, according to the same survey.[31] This creates yet another vector for the CCP through which to expand its influence over the cognitive landscape of the American body politic.

In one example of these soft influence operations against U.S. users, former ByteDance employees alleged in 2022 that TikTok's parent company deliberately served pro-China content to a U.S. audience through its old news app, TopBuzz, in addition to censoring stories unfavorable to the Chinese government.[32] In 2020, TikTok confirmed that the Chinese government asked its employees to set up an account, under the radar, that "[showcases] the best side of China (some sort of propaganda)," according to a TikTok employee.[33] Leaked documents revealed that TikTok censors content that exposes the CCP's genocide against its Uyghur community in the Xinjiang region and videos about Tiananmen Square, Tibetan independence, and Hong Kong protests.[34] Concurrently, TikTok accounts linked to Chinese

state media pushed divisive content to users during the 2022 U.S. midterm elections focusing on cultural flashpoints, such as the abortion debate, and mostly criticizing Republican candidates while favoring Democrats.[35]

TikTok's algorithm and unique technical features, such as "heating," or artificially picking stories to go viral, also facilitate its manipulation of the information environment.[36] Since the algorithm trains on data drawn from individual user preferences and engagement versus connections and "friend" networks, it amounts to a more bespoke vector for propaganda delivery. When information is tailored to individuals based on their unique digital profiles, it could supercharge, at scale, custom CCP influence operations against U.S. citizens.[37] It is not hard to envision how these techniques could be deployed for the next U.S. presidential election in 2024.

The Long Game: Integrating TikTok Data with Stolen Datasets to Map U.S. Networks and Life Patterns

Americans should be concerned about the integration of TikTok data with China's growing trove of stolen datasets from hacks conducted at least as far back as 2014. Seemingly disparate datasets, once integrated, can help foreign adversaries to create profiles of American citizens that are ripe for blackmail, espionage, and more.

TikTok data, if fused with other information, could paint comprehensive intelligence pictures of American users. This type of data integration involves bringing together distinct data sources and synthesizing them into something new and more useful than the constituent sources. Such integration can also be as simple as cross-referencing data to make inferences and assessments.

Relatedly, China's strides in AI development indicate that the Chinese party-state can and will apply emerging technologies to such datasets to expeditiously exploit its collection. Leveraging applications of AI, such as machine learning, and analytics can transform data into insights. These technologies can parse through raw data at machine speed and make it useful, such as by identifying patterns and anomalies or predicting and mapping trends. Big data analytics can help to process and analyze large volumes of data and extract meaning or flag items of interest. With the advent of these technologies, data that was previously discarded or ignored now has value. What TikTok collects is thus even more useful to the PRC.

China is no stranger to employing these techniques. In fact, CCP officials are already using analytics and data integration to enforce internal control in places like the Xinjiang Uyghur Autonomous Region using an "Integrated

Joint Operations Platform."[38] Through this and other systems, Chinese authorities aggregate behavioral and biometric data, such as whether its inhabitants use an abnormal amount of electricity, display religious enthusiasm, or fail to show up to the local CCP activity of the day.[39] Authorities collect iris scans, cheek swabs, eyelash and voice samples, and even 360 degree captures of an individual's gait, all with the intent of integrating these pieces of data to create a multimodal profile of individuals and identify potential threats to the regime.[40] TikTok—given the depth and scope of data it collects—could be used by the Chinese government to build digital profiles, determine patterns of life, and even map out the social networks of Americans.

The CCP can easily construct digital profiles of Americans using the surveillance footholds it has already gained in the United States and other parts of the West. China reportedly created dossiers on prominent Americans and those hailing from allied countries like Australia, Canada, and Great Britain as recently as 2020 with both stolen and publicly available datasets.[41] This is just the tip of the iceberg. The CCP could add TikTok and other "open-source" data to cross-reference data from the Chinese hack of the Office of Personnel Management detected in 2014, which exposed the Social Security numbers, addresses, and family contacts of thousands of U.S. government employees, among other sensitive information.[42] This data can be added to that from other hacks linked to the Chinese state, such as the hack of the Marriott hotel system in 2018, the Anthem health care system hack from 2015 and the Equifax financial services hack in 2017 to enable the CCP to track where U.S. citizens stay, who they travel with, and any vulnerabilities in their health, medical, or financial lives.[43] Patterns of life from digital platforms like TikTok, with real-time GPS and biometric data-collection capabilities, can fill in many gaps. As former Google CEO Eric Schmidt warns in a 2023 *Foreign Affairs* essay:

> [T]he warfare of the future will target individuals in completely new ways: authoritarian states such as China and Russia may be able to collect individual data on Americans' shopping habits, location, and even DNA profiles, allowing for tailor-made disinformation campaigns and even targeted biological attacks and assassinations.[44]

The Chinese party-state has already unleashed an advanced surveillance state on its own people. All efforts by the CCP to apply its surveillance apparatus to Americans must be actively repudiated.

Recommendations for the United States

Given the current threat environment, The Heritage Foundation recommends a wholesale ban of TikTok's operations in the United States (and, eventually, all U.S. allied countries). After implementing a U.S. ban, the federal government should craft, publicize, and enforce a risk framework for foreign-owned platforms and applications seeking entry into the U.S. market.[45] A systemic approach is required to prevent another TikTok from infiltrating America in the future.[46]

To achieve this outcome, Congress, along with the executive branch and relevant agencies, should:

Ban TikTok from Operating in the U.S. Market. Congress should eliminate the loophole that prevents the President from enforcing sanctions against TikTok. To do so, U.S. legislators should update the International Emergency Economic Powers Act's (IEEPA's) Berman Amendment. IEEPA generally grants the President broad authority to contend with unusual or extraordinary foreign threats through measures like economic sanctions or embargoes.[47] A 2020 executive order by President Trump attempted to use IEEPA authorities to ban TikTok as a national security threat.[48] TikTok sued the Trump Administration that same year and a federal judge sided with TikTok by relying in part on a loophole for "informational materials" in the Berman Amendment, which is a set of amendments to IEEPA originally meant to protect the free flow of legitimate communication, such as films and photographs, to the United States from hostile nations like Cuba.[49]

Congress should update the statute to account for today's information environment and data exploitation practices by foreign-owned digital platforms and their proxies.[50] Specifically, the informational materials exemption could be qualified with language to indicate that these materials should be reasonably free from malign state actor links and influence. TikTok, by virtue of its parent company ByteDance, would not meet this criterion for exemption.[51]

- Congress can make clear, for example, that under such an update to the Berman Amendment, the President can deem these foreign-owned digital platforms (1) a national security threat, and (2) under the influence of a malign state actor. Alternatively, Congress can find that TikTok already qualifies as a national security threat under malign state actor influence.

- Legislators can also engineer a ban through other avenues that eliminate the Berman Amendment loophole or otherwise allow the use of IEEPA authorities to ban TikTok. Such efforts include Senator Marco Rubio's (R–FL) draft bill Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party (ANTI-SOCIAL CCP) Act, a bipartisan companion bill in the House sponsored by Representatives Mike Gallagher (R–WI) and Raja Krishnamoorthi (D–IL), and Representative Mike McCaul's (R–TX) Deterring America's Technological Adversaries (DATA) Act.[52]

Institute a Risk-Based Framework that Triggers Specific Policies for Foreign-Owned Digital Platforms that Want to Operate in the United States. A solution to the next TikTok exists in a country-neutral risk framework applied to foreign-owned platforms.[53] When met, these criteria would trigger an if–then ruleset for more focused policy prescriptions. *If* a particular criterion or set of criteria is met, *then* a particular policy action should be enacted.[54] The Treasury Department, Commerce Department, State Department, and the National Institute of Standards and Technology can contribute to the development of this framework. Essential elements of risk-based criteria that, when met, should trigger specific policy action include:[55]

- **The digital platform's target audience and monthly active users** (such as the size of the digital platform's American userbase and scale of growth). Meeting high-risk criteria under this description would not trigger a specific policy action but would help to inform the next three criteria.

- **The platform's overall security** (such as vulnerability to hard security problems like hacking and intrusion). Meeting high-risk criteria under this description would likely trigger a CFIUS review.

- **The platform's collection and information-control practices** (such as features of its algorithms, content moderation, and censorship policies). Meeting high-risk criteria under this description would likely trigger the use of IEEPA sanctions.

- **The platform's home jurisdiction.** This last element should encompass a foreign government's data practices (that is, asking: Does the

foreign government use AI-driven systems for surveillance that data collection from a U.S. market will help to improve?), the foreign government's human rights record, and the foreign government's governance atmosphere.[56] Platforms emanating from adversary nations like Iran, North Korea, or Russia would effectively trigger specific policy action.[57] Meeting specific high-risk criteria in this description would likely trigger a combination of CFIUS review and Leahy Law restrictions.

Pass a National Data-Protection Framework to Address Third-Party Data Collection and Sharing Mechanisms for U.S. Users. Congress should prohibit digital applications from sending U.S. user data to TikTok/ByteDance and similar foreign-owned digital platforms that represent legitimate national security threats to the United States.

- A TikTok ban is not sufficient to protect U.S. data because myriad apps and trackers can send U.S. data to TikTok even if a user has not downloaded the TikTok app.[58] In the future, *if* a company like TikTok/ByteDance meets specific high-risk criteria under the risk-based framework proposed in this *Backgrounder*, *then* these apps should be prevented from sending U.S. data to these designated companies.

- Congress can take steps to prevent applications from providing TikTok, and therefore ByteDance, with U.S. data via a data-protection framework with appropriate standards and oversight for how commercial entities collect, store, and share U.S. user data.[59]

Private companies should:

Remove TikTok from Their App Stores While Congress Negotiates a Solution to the TikTok Problem. Pending congressional action on TikTok, U.S. tech companies, including Google and Apple, should remove TikTok from their app stores due to its relationship to the CCP and legitimate threat to national security.[60]

Conclusion

Every day that TikTok is allowed to operate in the United States is another day that China can collect information about U.S. citizens and sharpen its ability to exploit Americans—especially the young. The more that TikTok becomes embedded in the United States, the harder it will be to uproot.

Even so, there will be another TikTok. Without implementing a systemic, risk-based framework to proactively address the next TikTok now, the U.S. will have ceded yet another critical digital battlespace to its adversaries. More so, U.S. policymakers have a duty to safeguard America's social fabric and protect young citizens from the whims of an adversary nation. Failing to deliver means that the next generation of Americans will pay the price for Washington's lassitude.

Kara Frederick is Director of the Technology Policy Center at The Heritage Foundation.

Endnotes

1. "TikTok Owner ByteDance Increases Price of Stock Option Buyback," Reuters, October 12, 2022, https://www.reuters.com/technology/TikTok-owner-ByteDance-increases-price-share-buyback-staff-sources-2022-10-12/ (accessed March 11, 2023); "TikTok Hits 3 Billion Downloads," CNET, July 14, 2021, https://www.cnet.com/tech/services-and-software/TikTok-hits-3-billion-downloads/ (accessed March 11, 2023); Sarah Perez, "Kids and Teens Now Spend More Time Watching TikTok than YouTube, New Data Shows," TechCrunch, July 13, 2022, https://techcrunch.com/2022/07/13/kids-and-teens-watch-more-TikTok-than-youtube-TikTok-91-minutes-in-2021-youtube-56/ (accessed March 11, 2023); "BTN Newsbreak," Australian Broadcast Corporation, March 2, 2023, https://www.abc.net.au/btn/newsbreak/btn-newsbreak-20230302/102045772 (accessed March 14, 2023); Drew Harwell, "How TikTok Ate the Internet," *The Washington Post*, October 14, 2022, https://www.washingtonpost.com/technology/interactive/2022/TikTok-popularity/ (accessed March 10, 2023); and "Watch Live: Sen. Warner Holds Press Briefing on TikTok," *The Hill*, March 7, 2023, video, https://thehill.com/homenews/3888161-watch-live-sen-warner-holds-press-briefing-on-TikTok/ (accessed March 10, 2023).
2. Murray Scot Tanner, "National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (accessed March 10, 2023). See also the following excerpt from the author's 2019 white paper for the U.S. Cybersecurity Solarium Commission, with language from the author's 2019 testimony in front of the U.S. Senate Judiciary Subcommittee on Crime and Terrorism: Another similar policy is China's 2017 Cybersecurity Law, which is broadly written and provides a low threshold for access to data by the state. "[T]he CAC [Cyberspace Administration of China] updated the law in May 2019 to include a 'Data Security Management Measures' document, complete with 'personal information protection' and provisions for AI-driven content. Previous versions of the law invoke 'critical information infrastructure' and define 'network operators' in broad terms that extend beyond internet service providers to any entity using information and communication technologies (ICTs). As public policy researchers teased out for American media, these laws '[entail] strict provisions requiring data to be housed inside China, as well as spot inspections and even black-box security audits.' Finally, China's full 'internet security plan,' encompassing a soon-to-be-implemented 2020 Foreign Investment Law, will no longer render foreign-owned companies in China exempt from the Cybersecurity Law. Effectively, any data on communications networks in China will soon be subject to the Chinese Cybersecurity Bureau's scrutiny, without requiring an official request. This ability to access more data from more sources lays the groundwork for its exploitation." Kara Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Tesitmony1.pdf (accessed March 20, 2023).
3. Tanner, "National Intelligence Law: From Defense to Offense."
4. Ryan McMorrow, Qianer Liu, and Cheng Leng, "China Mes to Take 'Golden Shares' in Alibaba and Tencent Units," *Financial Times*, January 12, 2023, https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de (accessed March 20, 2023).
5. Coco Feng, "Chinese Government Takes Minority Stake, Board Seat in TikTok Owner ByteDance's Main Domestic Subsidiary," *South China Morning Post*, August 17, 2021, https://www.scmp.com/tech/big-tech/article/3145362/chinese-government-takes-minority-stake-board-seat-tiktok-owner (accessed March 14, 2023), and "Exclusive: Fretting About Data Security, China's Government Expands Its Use of 'Golden Shares,'" Reuters, December 16, 2021, https://www.reuters.com/markets/deals/exclusive-fretting-about-data-security-chinas-government-expands-its-use-golden-2021-12-15/ (accessed March 14, 2023).
6. U.S. Department of Justice, "Defendants' Memorandum in Opposition to Plaintiffs' Motion for a Preliminary Injunction," September 25, 2020, https://www.documentcloud.org/documents/7218230-DOJ-s-MEMORANDUM-in-OPPOSITION-to-TIKTOK.html (accessed March 10, 2023).
7. Emily Baker-White, "LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—and Some Still Do," *Forbes*, August 11, 2022, https://www.forbes.com/sites/emilybaker-white/2022/08/10/ByteDance-TikTok-china-state-media-propaganda/?sh=68359903322f (accessed March 10, 2023).
8. Ibid.
9. Chris Stokel-Walker, "Inside TikTok's Attempts to 'Downplay the China Association,'" *Gizmodo*, July 27, 2022, https://gizmodo.com/TikTok-master-messaging-pr-playbook-china-music-1849334736 (accessed March 10, 2023).
10. Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," Center for a New American Security, September 3, 2020, https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem (accessed March 12, 2023).
11. TikTok, "Privacy Policy," January 1, 2023, https://www.tiktok.com/legal/page/us/privacy-policy/en (accessed March 20, 2023).
12. TikTok, "Privacy Policy," and Paul Mozur, Ryan Mac, and Chang Che, "TikTok Browser Can Track Users' Keystrokes, According to New Research," *The New York Times*, August 29, 2022, https://www.nytimes.com/2022/08/19/technology/TikTok-browser-tracking.html (accessed March 10, 2023).
13. David Robinson, "TikTok Scores 63.1—Designed to Collect Data with Highest Malcore Score in Industry," Malcore, February 13, 2023, https://blog.malcore.io/p/TikTok-scores-631-designed-to-collect (accessed March 10, 2023).
14. Ibid.
15. Kevin Poulsen and Robert McMillan, "TikTok Tracked User Data Using Tactic Banned by Google," *The Wall Street Journal*, August 11, 2020, https://www.wsj.com/articles/TikTok-tracked-user-data-using-tactic-banned-by-google-11597176738 (accessed March 10, 2023).

16. Ibid.
17. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 40, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023).
18. Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China," *BuzzFeed News*, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-tapes-us-user-data-china-ByteDance-access (accessed March 10, 2023).
19. Kurt Zindulka, "Former MI6 Chief: TikTok Gives CCP a Backdoor into Politicians' Data," *Breitbart*, August 12, 2020, https://www.breitbart.com/europe/2020/08/11/former-mi6-chief-TikTok-gives-ccp-a-backdoor-into-politicians-data-through-their-kids-smartphone/ (accessed March 10, 2023).
20. Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China."
21. Ibid.
22. Roland Cloutier, "Our Approach to Security," TikTok, April 28, 2020, https://newsroom.TikTok.com/en-us/our-approach-to-security (accessed March 10, 2023).
23. Josh Hawley, letter to Janet Yellen, March 7, 2023, https://www.documentcloud.org/documents/23698254-2023-03-07-hawley-letter-to-yellen-TikTok (accessed March 10, 2023).
24. Emily Baker-White, "Exclusive: TikTok Spied on Forbes Journalists," *Forbes*, December 2, 2022, https://www.forbes.com/sites/emilybaker-white/2022/12/22/TikTok-tracks-forbes-journalists-ByteDance/?sh=55bb707e7da5 (accessed March 10, 2023).
25. Ibid.
26. Liza Lin and Raffaele Huang, "TikTok's Talks with U.S. Have an Unofficial Player: China," *The Wall Street Journal*, February 14, 2023, https://www.wsj.com/articles/TikToks-talks-with-u-s-have-an-unofficial-player-china-f5fec4ec (accessed March 10, 2023).
27. Aaron Tilley, "TikTok Says All Data for U.S. Users Now Routed to Oracle Cloud," *The Wall Street Journal*, June 17, 2022, https://www.wsj.com/articles/TikTok-says-all-data-for-u-s-users-now-routed-to-oracle-cloud-11655503707 (accessed March 12, 2023); Jonathan Cheng, "Chinese State Television: 'ByteDance Will Not Sell TikTok's U.S. Operations to Microsoft or Oracle, nor Will the Company Give the Source Code to Any U.S. Buyers, Sources Said,'" Twitter, September 14, 2020, https://twitter.com/jchengwsj/status/1305381978422812673 (accessed March 10, 2023), and Georgia Wells and Aaron Tilley, "Oracle Wins Bid for TikTok in U.S., Beating Microsoft," *The Wall Street Journal*, September 14, 2020, https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-TikToks-u-s-operations-11600039821 (accessed March 10, 2023).
28. Christopher Wray, "2022 Josh Rosenthal Memorial Talk," The Ford School at the University of Michigan, December 2, 2022, https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk (accessed March 10, 2023).
29. Ivana Saric, "China Could Use TikTok to Control Users' Devices, FBI Director Says," Axios, March 8, 2023, https://www.axios.com/2023/03/08/china-TikTok-fbi-director-congress (accessed March 10, 2023).
30. Katerina Eva Matsa, "More Americans Are Getting News on TikTok, Bucking the Trend on Other Social Media Sites," Pew Research Center, October 21, 2022, https://www.pewresearch.org/fact-tank/2022/10/21/more-americans-are-getting-news-on-TikTok-bucking-the-trend-on-other-social-media-sites/ (accessed March 10, 2023).
31. Ibid.
32. Emily Baker-White, "TikTok Owner ByteDance Used a News App on Millions of Phones to Push Pro-China Messages, Ex-Employees Say," *Buzzfeed News*, July 26, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-ByteDance-topbuzz-pro-china-content (accessed March 10, 2023).
33. Olivia Solon, "Chinese Government Asked TikTok for Stealth Propaganda Account," Bloomberg, July 29, 2022, https://www.bloomberg.com/news/articles/2022-07-29/chinese-government-asked-TikTok-for-stealth-propaganda-account?leadSource=uverify%20wall (accessed March 12, 2023), and Drew Harwell and Tony Room, "TikTok's Beijing Roots Fuel Censorship Suspicion as it Builds a Huge U.S. Audience," *The Washington Post*, September 15, 2019, https://www.washingtonpost.com/technology/2019/09/15/TikToks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/ (accessed March 10, 2023).
34. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 15, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023), and Alex Hern, "Revealed: How TikTok Censors Videos that Do Not Please Beijing," *The Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-TikTok-censors-videos-that-do-not-please-beijing (accessed March 10, 2023).
35. Emily Baker-White and Iain Martin, "On TikTok, Chinese State Media Pushes Divisive Videos about U.S. Politicians," *Forbes*, December 1, 2022, https://www.forbes.com/sites/emilybaker-white/2022/11/30/TikTok-chinese-state-media-divisive-politics (accessed March 10, 2023).
36. Emily Baker-White, "TikTok's Secret 'Heating' Button Can Make Anyone Go Viral," *Forbes*, January 20, 2023, https://www.forbes.com/sites/emilybaker-white/2023/01/20/TikToks-secret-heating-button-can-make-anyone-go-viral (accessed March 10, 2023).

37. Michael Horowitz et al., "Artificial Intelligence and International Security," Center for a New American Security, July 10, 2018, https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security (accessed March 10, 2023); Jordan Schneider, "What to Do About TikTok and WeChat," *ChinaTalk*, July 20, 2020, https://chinatalk.substack.com/p/what-to-do-about-TikTok (accessed March 12, 2023); and Brit McCandless Farmer, "How TikTok Could Be Used for Disinformation and Espionage," CBS News, November 15, 2020, https://www.cbsnews.com/news/TikTok-disinformation-espionage-60-minutes-2020-11-15/ (accessed March 10, 2023).
38. Australian Strategic Policy Institute, "How Mass Surveillance Works in Xinjiang: Reverse Engineering the Police Mass Surveillance App," April 2019, https://xjdp.aspi.org.au/explainers/how-mass-surveillance-works-in-xinjiang/ (accessed March 16, 2023), and Human Rights Watch, "China's Algorithms of Repression," May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass (accessed March 12, 2023).
39. Human Rights Watch, "China's Algorithms of Repression," and Yael Grauer, "Revealed: Massive Chinese Police Database," The Intercept, January 29, 2021, https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/ (accessed March 16, 2023).
40. Megan Rajagopalan, "They Thought They'd Left the Surveillance State Behind. They Were Wrong," BuzzFeed, July 9, 2018, https://www.buzzfeednews.com/article/meghara/china-uighur-spies-surveillance (accessed March 12, 2023).
41. Andrew Probyn and Matthew Doran, "China's 'Hybrid War': Beijing's Mass Surveillance of Australia and the World for Secrets and Scandal," Australian Broadcasting Corporation, September 13, 2020, https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668 (accessed, March 10, 2023).
42. Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," CNN, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html (accessed March 10, 2023).
43. David E. Sanger et al., "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *The New York Times*, December 10, 2018, https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html (accessed March 10, 2023); Eric Geller, "Chinese Nationals Charged for Anthem Hack, 'One of the Worst Data Breaches in History,'" *Politico*, May 9, 2019, https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341 (accessed March 10, 2023); and Federal Bureau of Investigation, "Chinese Military Hackers Charged in Equifax Breach," February 10, 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020 (accessed March 10, 2023).
44. Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs*, February 28, 2023, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics (accessed March 10, 2023).
45. Kara Frederick, Chris Estep, and Megan Lamberth, "Beyond TikTok: Preparing for Future Digital Threats," *War on the Rocks*, August 20, 2020, https://warontherocks.com/2020/08/beyond-TikTok-preparing-for-future-digital-threats/ (accessed March 3, 2023).
46. Kara Frederick, "Democracy by Design," Center for a New American Security, December 15, 2020, https://www.cnas.org/publications/reports/democracy-by-design (accessed March 3, 2023).
47. 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act.
48. The White House, "Executive Order on Addressing the Threat Posed by TikTok," August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-TikTok/ (accessed March 10, 2023).
49. John D. McKinnon, "TikTok Ban Faces Obscure Hurdle: The Berman Amendments," *The Wall Street Journal*, January 29, 2023, https://www.wsj.com/articles/tiktok-ban-faces-obscure-hurdle-the-berman-amendments-11674964611 (accessed March 14, 2023); *TikTok., Inc., et al., v. Donald J Trump*, Civil Action No. 1:20-cv-02658 [federal court], https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv2658-30 (accessed March 20, 2023); 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act; and Christopher A. Casey et al., "The International Emergency Economic Powers Act: Origins, Evolution, and Use," Congressional Research Service R45618, July 14, 2020, https://fas.org/sgp/crs/natsec/R45618.pdf (accessed March 17, 2023). As researchers at the Center for a New American Security highlighted in a 2021 report, any presidential Administration's "hands are effectively tied…when it comes to using IEEPA to address the national security concerns associated with social media applications and websites" due to the Berman Amendment's exemption for "informational materials."
50. John Costello, Martijn Rasser, and Megan Lamberth, "From Plan to Action: Operationalizing a U.S. National Technology Strategy," Center for a New American Security, July 29, 2021, https://www.cnas.org/publications/reports/from-plan-to-action (accessed March 10, 2023).
51. Other proposals, such as the Data and Algorithm Transparency Agreement (DATA) Act, suggest exempting "sensitive personal data" from Berman Amendment protections.
52. Marco Rubio and Mike Gallagher, "TikTok, Time's Up. The App Should Be Banned in America," *The Washington Post*, November 10, 2022, https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-TikTok-america-china-mike-gallagher/ (accessed March 10, 2023); The White House "Executive Order on Addressing the Threat Posed by TikTok"; David Feith, "Opportunities and Challenges for Trade Policy in the Digital Economy," Center for a New American Security, November 30, 2022, https://www.cnas.org/publications/congressional-testimony/opportunities-and-challenges-for-trade-policy-in-the-digital-economy (accessed March 10, 2023); and Brendan Bordelon, "GOP Rams Through TikTok Ban Bill Over Dem Objections," *Politico*, March 1, 2023, https://www.politico.com/news/2023/03/01/house-republicans-TikTok-ban-00084951 (accessed March 2023).
53. This concept of systemic risk and a risk-based framework with a ruleset to contend with future challenges is derived from the author's previous publications and communications with Administration officials and journalists starting in 2019, including but not limited to: Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem"; Frederick, "Democracy by Design"; Frederick, Estep, and Lamberth, "Beyond TikTok: Preparing

for Future Digital Threats"; Kara Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Tesitmony1.pdf (accessed March 20, 2023); and David Wertime, "America's Problem Is Much Bigger than TikTok," *Politico*, September 3, 2020, https://www.politico.com/newsletters/politico-china-watcher/2020/09/03/beijing-washington-next-TikTok-data-rules-standards-490242 (accessed March 10, 2023).

54. These policy actions can be a combination of tools already in the U.S. government policy toolkit, such as IEEPA sanctions, Leahy Law restrictions, or CFIUS reviews.
55. Derived from the author's e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher. Wertime, "America's Problem Is Much Bigger than TikTok."
56. From the author's e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher: "A governance atmosphere encompasses the systemic risk a nation brings to the table through its political institutions and legal environment (e.g. China's national intelligence law, Hong Kong's national security law, etc). This would control for the lack of recourse against government demands for private data, information, and/or access, like an independent judiciary and free press." And from Frederick, "The Razor's Edge": "For instance, China lacks sufficient rule-of-law protections, specific corporate governance practices, and democratic features that would allow companies to resist arbitrary requests for information from the Chinese government." Also see Frederick, "Democracy by Design."
57. This concept is not unlike the U.S. State Department's annual International Religious Freedom report's "Countries of Particular Concern" designations that lead to specific policy action.
58. Thomas Germain, "How TikTok Tracks You Across the Web, Even If You Don't Use the App," *Consumer Reports*, September 29, 2022, https://www.consumerreports.org/electronics-computers/privacy/TikTok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/ (accessed March 10, 2023).
59. Kara Frederick, "Combating Big Tech's Totalitarianism: A Road Map," Heritage Foundation *Backgrounder* No. 3678, February 7, 2022, https://www.heritage.org/technology/report/combating-big-techs-totalitarianism-road-map.
60. Brendan Carr, Commissioner of the Federal Communications Commission, letter to Apple and Google, June 24, 2023, https://www.fcc.gov/sites/default/files/carr-letter-apple-and-google.pdf (accessed March 10, 2023).